SECURITY MANUAL

Biopharmaceutical industry practices

ONCOSHOT

https://www.oncoshot.com

CONTENTS

01 The Importance of Data Security in the Biopharmaceutical Industry

02 Overview of Key Data Privacy Regulations Worldwide

03 Overview of Industry Accreditations and Qualifications

04 Oncoshot Data Security Practices

05 Oncoshot Compliance with Regulations and Standards

THE IMPORTANCE OF DATA SECURITY IN THE BIOPHARMACEUTICAL INDUSTRY

Data security in the biopharmaceutical industry is crucial due to the sensitive nature of patient health records, clinical trial data, and proprietary research information involved. Protecting this data from breaches and unauthorized access maintains patient privacy, scientific integrity, and intellectual property.

Regulations like GDPR and HIPAA enforce stringent data handling, storage, and sharing standards. Compliance avoids penalties and fosters trust.

Certifications like ISO 27001, ISO 27017 and SOC 2 provide frameworks for robust information security management systems. Together, these regulations and certifications critically defend against cyberattacks and data breaches, safeguarding individual privacy and biopharmaceutical industry interests.

OVERVIEW OF KEY DATA PRIVACY REGULATIONS WORLDWIDE

Health Insurance Portability and Accountability Act (HIPAA)

2003

Protection of Personal Healthcare Information

Singapore's Personal Data Protection Act (PDPA)

2012

Recognizes individual control over their personal data and regulates organizations' handling of personal information

EU General Data Protection Regulation (GDPR)

2018

Standardizes Privacy Protection Practices for EU Citizens

California Consumer Privacy Act (CCPA)

2020

Regulates companies and individuals collecting and processing consumer personal information

Health Insurance Portability and Accountability Act (HIPAA)

Protection of Personal Healthcare Information

Key Highlights:

Privacy Protection Rules

Privacy protection rules are established to specify principles governing the use and disclosure of Protected Health Information (PHI).

Collaborative Partner Contracts

Collaborative partner contracts outline written guidelines for the use, protection, and disclosure of data.

Singapore's Personal Data Protection Act (PDPA)

Recognizes individual control over their personal data and regulates organizations' handling of personal information

Key Highlights:

Data Protection Principles

PDPA establishes rules for collecting, using, and disclosing personal data, including consent, purpose limitation, and data accuracy.

Consent Requirements

Clear consent is required before using personal data; individuals can withdraw consent anytime.

EU General Data Protection Regulation (GDPR)

Standardizes Privacy Protection Practices for EU Citizens

Key Highlights:

Personal Data Usage

Personal data, especially health data, should be used for specific purposes and within defined scopes, requiring individual consent.

Individual Rights

Individuals can access information about their data collection rights under the law.

California Consumer Privacy Act (CCPA)

Regulates companies and individuals collecting and processing consumer personal information

Key Highlights:

Data Access Rights

Individuals can request information about the collection of their personal data as defined by CCPA.

Privacy Control

CCPA grants individuals control over their personal information, allowing them to access and manage how it's used.

OVERVIEW OF INDUSTRY ACCREDITATIONS AND QUALIFICATIONS

ISO 27001

ISO 27001 is the international standard that specifies the requirements for an information security management system (ISMS).

ISO 27017

ISO 27017 provides security guidelines and controls tailored for cloud service providers to supplement the ISO 27001 standard.

ISO 27018

ISO 27018 is a code of practice that provides guidance on protecting personal data in public cloud computing environments as a supplement to ISO 27001.

SOC 2

SOC 2 is an auditing framework by the AICPA for evaluating an organization's data security, availability, processing integrity, confidentiality, and privacy controls.

ISO27001

Information Security Management System Certification

An internationally recognized standard for information security management systems

Most biopharmaceutical companies worldwide have passed this certification

ISO27017

Security standard developed for cloud service providers and users

Widely Acknowledged. Acknowledged as a standard for cloud information security management, fostering trust and credibility worldwide.

Strong Protection. Provides robust protection of personal data in cloud systems, minimizing risks and enhancing compliance.

ISO27018

Public Cloud Personally Identifiable Information Management System Certification

An internationally recognized standard for managing the protection of personally identifiable information in the cloud

Meets the requirements of sponsors and regulators for the protection of personal information in biopharmaceutical companies

SOC 2

Service Organization Control
Type 2

SOC 2 – is a cybersecurity framework developed by the American Institute of Certified Public Accountants (AICPA) in 2010

SOC 2 provides a framework for service organizations to obtain an independent assessment of their control environment relevant to security, availability, processing integrity, confidentiality, and privacy

Oncoshot Data Security Practices

ONCOSHOT

https://www.oncoshot.com

Data Encryption

Data encryption encodes data to prevent unauthorized access

Encryption in Transit

Encrypt data as it travels across networks to prevent interception

Encryption at Rest

Encrypt data stored on devices and servers to protect it from unauthorized access

Access Controls

regulate and restrict system access to authorized users, programs, or processes

Role-Based Access Control (RBAC)

Grant access based on user roles and job responsibilities, ensuring that individuals only have access to the information necessary for their role

Multi-Factor Authentication (MFA)

Require multiple forms of verification before granting access to systems and data

Strong Password Policies

Implement policies requiring strong, unique passwords and regular password changes

Regular Audits and Monitoring

Regular security audits and monitoring enable continuous compliance verification

Audit Trails

Maintain detailed logs of access and activity within healthcare systems to track and review actions taken by users

Continuous Monitoring

Implement real-time monitoring to detect and respond to suspicious activities and potential security breaches

Network Security

Network security safeguards infrastructure and data transmissions from threats

Firewalls

Use firewalls to protect the internal network from external threats

Intrusion Detection and Prevention Systems (IDPS)

Deploy systems to detect and prevent unauthorized access and malicious activities

Virtual Private Networks (VPNs)

Use VPNs to secure remote access to healthcare systems

Physical Security

Controls restrict physical access to premises, equipment, and data storage

Restricted Access

Limit physical access to servers, data centers, and other critical infrastructure to authorized personnel only

Security Cameras and Alarms

Use surveillance systems and alarms to monitor and secure physical locations

Data Backup and Recovery

Data backup and recovery protects against data loss and threats, ensuring data restoration

Regular Backups

Perform regular backups of critical data to ensure it can be restored in the event of data loss or corruption

Disaster Recovery Plan

Maintain a comprehensive disaster recovery plan to ensure quick and effective recovery from major incidents

Employee Training and Awareness

Mitigates risks by ensuring staff are informed, skilled, and proactive in maintaining security and compliance

Security Training

Provide ongoing training for employees on security best practices, phishing awareness, and the importance of protecting patient information

Security Policies

Enforce clear security policies and procedures for handling sensitive data

Patch Management

Patch Management ensures systems remain secure and functional by regularly updating software to fix vulnerabilities and bugs

Regular Updates

Keep all software, systems, and devices up to date with the latest security patches and updates to protect against known vulnerabilities

Oncoshot Compliance with Regulations and Standards

Oncoshot certified for multiple international compliances which fulfilled the requirements of working in the HealthTech industry

ISO 27001

ISO 27017

ISO 27018

GENERAL DATA PROTECTION REGULATION ★★★★★ GDPR READY ✓

PERSONAL DATA PROTECTION ACT ★★★★★ PDPA COMPLIANCE ✓

AICPA Service Organization Control Reports AICPA SOC 2 Formerly SAS 70 Reports

HIPAA COMPLIANT HIPAATraining.com

aws PARTNER Public Sector

aws Qualified Software